Kaspersky ICS CERT

kaspersky

APT-атаки на промышленные компании во второй половине 2022 года

24.03.2023

Version 1.0

Юго-Восточная Азия и Корейский полуостров 2
Атаки DEV-0530 2
Атаки Tropic Trooper 2
Атаки семейства программ-вымогателей GwisinLocker 3
Атаки Lazarus 4
Атаки UNC4034/ZINC 6
Ближний Восток 6
Атаки UNC3890 6
Атаки POLONIUM 7
Активность китайскоязычных групп 8
Атаки TA428 8
Атаки APT31 9
Атаки TA423/Red Ladon 9
Шпионаж за государственными организациями стран Азии 10
Атаки Budworm 10
Атаки Earth Longzhi 11
Активность русскоговорящих групп 12
Атаки IRIDIUM/Sandworm 12
Атаки Cloud Atlas/Inception 12
Другие атаки 13
Атаки Woody Rat 13
Атаки Worok 13
Бюллетени CISA 14
APT-группы с поддержкой Ирана 14
Взлом систем оборонного подрядчика 15

Эта подборка представляет собой обзор APT-атак на промышленные предприятия, информация о которых была раскрыта во втором полугодии 2022 года, и связанной с этим активности групп, замеченных в атаках на промышленные организации и объекты критической инфраструктуры. В каждом случае мы старались представить наиболее важные факты, результаты и выводы исследователей, которые, по нашему мнению, могут быть полезны экспертам, решающим практические вопросы обеспечения кибербезопасности промышленных предприятий.

Юго-Восточная Азия и Корейский полуостров

Атаки DEV-0530

Исследователи атрибутировали новую угрозу, связанную с программами-вымогателями, северокорейской группе злоумышленников, которую они назвали DEV-0530 (сама группа называет себя “H0lyGh0st”). С сентября 2021 года DEV-0530 проводит в нескольких странах атаки на организации малого и среднего бизнеса, включая производственные организации, банки, школы и компании, занимающиеся организацией мероприятий и встреч. Злоумышленники прибегают к «двойному вымогательству»: шифруют данные жертв, а также грозят опубликовать данные, если жертва откажется платить. Исследователи обнаружили связи DEV-0530 с APT-группой PLUTONIUM (она же DarkSeoul и Andariel).

В период с июня 2021 года по май 2022 года Центр киберразведки Microsoft (Microsoft Threat Intelligence Center, MSTIC) классифицировал программы-вымогатели H0lyGh0st как принадлежащие двум новым семействам вредоносного ПО: SiennaPurple и SiennaBlue. Исследователи подозревают, что DEV-0530 использовала для первичного доступа в целевые сети такие уязвимости как CVE-2022-26352 (уязвимость DotCMS, дающая возможность удаленного выполнения кода) в публичных веб-приложениях и системах управления контентом.

Атаки Tropic Trooper

Более десяти лет APT-группа Tropic Trooper активно атаковала жертв из Восточной и Юго-Восточной Азии. «Лаборатория Касперского» уже несколько лет отслеживает деятельность этой группы и выпустила отчет с описанием ее вредоносной активности, доступный по подписке на сервис Threat Intelligence Reporting.

В феврале 2022 года компания Symantec опубликовала отчет с описанием кампании, получившей название Antlion. В ходе кампании злоумышленники атаковали финансовые организации на Тайване, а также производственную компанию, присутствие в которой они сохраняли около 175 дней. В случае производственной компании исследователи наблюдали, как злоумышленники пытались загрузить вредоносные файлы, используя доступ по протоколу SMB. Эксперты «Лаборатории Касперского» при анализе индикаторов заражения этой кампании обнаружили тесные связи с группой злоумышленников Tropic Trooper и пришли к выводу, что эта группа стояла за кампанией Antlion.

В ходе расследования «Лаборатории Касперского» были обнаружены и изучены различные атаки, проведенные этой группой злоумышленников с применением семейств вредоносного ПО, описанных Symantec, а также новых версий вредоносного ПО, описанного в одном из предыдущих отчетов «Лаборатории Касперского» об APT-группе Tropic Trooper. В частности, были исследованы цепочки заражений при реализации этих атак, используемая злоумышленниками инфраструктура, развитие атаки и действия злоумышленников после внедрения в систему. Также были выявлены другие пострадавшие от атак отрасли помимо финансового сектора, включая высокотехнологичное производство оборудования и полупроводников и одну политическую организацию.

Более того, эксперты «Лаборатории Касперского» обнаружили ранее неизвестный модульный бэкдор, установленный на машине жертвы в августе 2021 года, использующий для сетевого взаимодействия с командным сервером протокол MQTT. При попытке проследить историю применения этого бэкдора выяснилось, что данная группа злоумышленников, по-видимому, применяла этот модуль как минимум с 2019 года, причем только в атаках на выбранные цели.

Атаки семейства программ-вымогателей GwisinLocker

Исследователи компании ReversingLabs обнаружили новое семейство программ-вымогателей, заражающих системы на основе ОС Linux с функционалом, специально предназначенным для работы и взаимодействия с виртуальными машинами VMWare ESXI. Вредоносное ПО, получившее название GwisinLocker, было обнаружено в успешных кампаниях, в ходе которых были атакованы промышленные и фармацевтические фирмы из Южной Кореи.

Анализ и публичные отчеты по всей широкомасштабной кампании GwisinLocker указывают на то, что вредоносные программы-вымогатели находятся в руках квалифицированных злоумышленников, которые получают доступ к инфраструктуре атакуемых компаний до размещения в ней программ-вымогателей и крадут конфиденциальные данные, которые затем применяются в кампаниях, использующих тактику «двойного вымогательства». Особенности оставляемых группой сообщений с требованием выкупа свидетельствуют о знании корейского языка, а также особенностей системы государственной власти и правоохранительных органов Южной Кореи. Исходя из этого можно предположить, что, возможно, злоумышленники принадлежат к APT-группе, имеющей связи с Северной Кореей.

Атаки Lazarus

Группа злоумышленников Lazarus использовала для целевых атак на инженеров подписанный вредоносный исполняемый файл для macOS, замаскированный под документ с описанием вакансии с именем файла Coinbase_online_careers_2022_07.pdf. Исполняемый файл, совместимый с процессорами производства как Apple, так и Intel, выглядит как описание вакансии инженера по обеспечению безопасности продуктов с Coinbase. Второй используемый злоумышленниками вредоносный исполняемый файл — это загрузчик, скачивающий вредоносную нагрузку второго этапа с удаленного сервера. Исследователи связали это вредоносное ПО с кампанией «Operation In(ter)caption», проводимой группой Lazarus против крупных игроков аэрокосмической и оборонной отраслей.

DTrack — бэкдор, применяемый подразделениями группы Lazarus. Он был использован в разных атаках, включая атаки вредоносных программ-вымогателей и кампании кибершпионажа. Специалисты «Лаборатории Касперского» обнаружили и исследовали новые образцы DTrack. Эти новые образцы иначе упакованы при относительно незначительных изменениях в коде. В публичном отчете дан подробный анализ этого нового набора образцов с описанием изменений и механизмов упаковки. Согласно телеметрии KSN, активность DTrack была обнаружена в Бразилии, Германии, Индии, Италии, Мексике, Саудовской Аравии, США, Турции и Швейцарии. Это показывает, что DTrack активно распространяется в разных частях света. Отмечены атаки на организации из следующих секторов: образование, химическая промышленность, государственные исследовательские центры и политические институты, провайдеры интернет-сервисов, коммунальные и телекоммуникационные компании.

Исследователи из Cisco Talos опубликовали отчет об атаках Lazarus на энергетические компании в США, Канаде и Японии. Атаки проводились в период с февраля по июль с целью кражи данных и информации, составляющей коммерческую тайну. Атаки начинаются с эксплуатации уязвимостей Log4j в VMware Horizon, после чего устанавливаются три специально созданных вредоносных импланта. Первый — VSingle — способен выполнять произвольный код из удаленной сети, а также загружать и запускать плагины. Второй — YamaBot — это специально созданный имплант на Golang, предназначенный для взаимодействия с командными серверами. Третий имплант — MagicRAT — это троянец удаленного доступа, запускающий дополнительные вредоносные нагрузки, такие как специально созданные сканеры портов.

Исследователи компании ESET обнаружили и проанализировали вредоносный инструментарий, использованный APT-группой Lazarus в атаках, которые проводились осенью 2021 года. Кампания началась с целенаправленной фишинговой рассылки, содержащей вредоносные документы на темы, связанные с компанией Amazon. Письма были отправлены сотруднику аэрокосмической компании из Нидерландов и бельгийскому политическому журналисту. Основной целью атакующих была кража данных. Наиболее интересный инструмент, примененный в данной кампании, связан с первым известным случаем эксплуатации уязвимости CVE-2021-21551 в драйверах Dell DBUtil. Этот метод — «прийти с собственным уязвимым драйвером» (Bring Your Own Vulnerable Driver, BYOVD) — был применен для отключения семи системных механизмов мониторинга Windows и «ослепления» защитных решений на взломанных машинах. Группа Lazarus также использовала в этой кампаний свой полнофункциональный HTTP(S) бэкдор под названием BLINDINGCAN.

Исследователи «Лаборатории Касперского» также обнаружили продолжающуюся с марта активную кампанию Lazarus, нацеленную на оборонных подрядчиков Южной Африки и Бразилии. Атакующие связывались с потенциальными жертвами через социальные сети или по электронной почте и отправляли им по Skype первоначальное вредоносное ПО — PDF-приложение с добавленным троянским функционалом. Это ПО запускает состоящую из нескольких этапов цепочку заражений, загружая дополнительные вредоносные нагрузки, содержащие функционал взаимодействия с командным сервером, с помощью механизма «боковой» загрузки DLL (DLL side-loading). Кроме того, атакующие устанавливали дополнительное вредоносное ПО на первоначальный хост для заражения новых машин и развития атаки. При этом использовалась относительно новая разновидность механизма «боковой» загрузки DLL, известная под названием ServiceMove. Этот метод был впервые применен исследователем из «red team», который использовал уязвимость в «Windows Perception Simulation Service» для загрузки произвольных DLL-файлов с вредоносными целями. Группа Lazarus имеет в своем арсенале различные инструменты и применяет их в разнообразных цепочках заражений. При анализе всех образцов, примененных в данной кампании, было отмечено вредоносное ПО из разных кластеров: ThreatNeedle, Bookcode и DeathNote.

Атаки UNC4034/ZINC

Исследователи из компании Mandiant обнаружили применение группой злоумышленников UNC4034 версий SSH-клиента PuTTY с внедренным в них троянским функционалом для установки на целевых устройствах бэкдора AIRDRY.V2. Эта активность выглядит как часть кампании Operation Dream Job, продолжающейся с июня 2020 года и связанной, по подозрениям экспертов, с Северной Кореей. Злоумышленники связываются с потенциальными жертвами, отправляя им электронное письмо с предложением высокооплачиваемой работы в компании Amazon, а затем переносят общение в мессенджер WhatsApp, через который пересылают ISO-файл, в состав которого входит файл readme с IP-адресом и учетными данными, а также версию PuTTY — популярного консольного приложения SSH с открытым исходным кодом — с внедренным в нее троянским функционалом.

Компания Microsoft отслеживает стоящую за этими атаками группу под именем ZINC. В своих атаках группа применяет ПО с открытым исходным кодом, в которое внедрен вредоносный функционал. Эксперты компании наблюдали активность группы, направленную против сотрудников организаций в различных секторах экономики, включая СМИ, оборонную и аэрокосмическую отрасли и ИТ-сервисы, из США, Великобритании, Индии и России. Известно, что группа ZINC при проведении описанных выше атак внедряла вредоносный функционал в самое разное ПО с открытым исходным кодом, включая PuTTY, KiTTY, TightVNC, Sumatra PDF Reader, а также инсталлятор ПО muPDF/Subliminal Recording.

Ближний Восток

Атаки UNC3890

Исследователи связали кластер вредоносной активности, который они считают иранским, с атаками на израильские организации, работающие в таких секторах как грузоперевозки, органы государственной власти, энергетика и здравоохранение. Эта кампания продолжается с конца 2020 года. По мнению экспертов, данные, собранные злоумышленниками в ходе этой кампании, могут быть использованы в различных видах вредоносной активности. Группа злоумышленников UNC3890, стоящая за этими атаками, применяла, в частности, две проприетарных вредоносных программы: бэкдор SUGARUSH и средство кражи учетных данных из браузеров SUGARDUMP, отправляющее украденные пароли на электронные адреса в

почтовых системах Gmail, ProtonMail, Yahoo и Яндекс. Кроме того, группа злоумышленников использует сеть командных серверов, на которых размещены фальшивые страницы якобы для входа на такие легитимные платформы как Office 365, LinkedIn и Facebook. Эти серверы взаимодействуют с жертвами атак, а также с ресурсом для проведения атаки типа watering hole, размещенным на странице входа на сайт легитимной израильской компании-грузоперевозчика.

Атаки POLONIUM

Исследователи обнаружили не документированные ранее нестандартные бэкдоры и средства кибершпионажа, применяемые APT-группой POLONIUM для атак на израильские цели. Среди целей этих атак организации в таких секторах как инжиниринг, ИТ, юриспруденция, связь, брендирование и маркетинг, СМИ, страхование и социальное обслуживание. В период с сентября 2021 года по сентябрь 2022 года группа злоумышленников атаковала более дюжины организаций.

Инструментарий POLONIUM состоит из семи нестандартных бэкдоров: CreepyDrive, который использует облачные сервисы OneDrive и Dropbox для организации командных серверов; CreepySnail, который выполняет команды, полученные из собственной инфраструктуры злоумышленников; DeepCreep и MegaCreep, которые используют, соответственно, сервисы хранения файлов Dropbox и Mega; а также FlipCreep, TechnoCreep и PapaCreep, которые получают команды с серверов злоумышленников. Группа создала также несколько нестандартных модулей для шпионажа за жертвами атак с помощью снимков экрана, регистрации нажатия клавиш, шпионажа через веб-камеру, открытия обратной оболочки, отправки украденных файлов и т.д. По словам исследователей, «большинство вредоносных модулей группы имеют маленький размер и ограниченную функциональность», например, «один модуль для снятия снимков экрана, другой для их загрузки на командный сервер». Злоумышленники любят разделять код, распределяя вредоносный функционал по нескольким маленьким DLL-файлам, возможно, в надежде, что специалисты по безопасности или исследователи не смогут проследить всю цепочку атаки.

Активность китайскоязычных групп

Атаки TA428

Эксперты Kaspersky ICS CERT обнаружили волну целевых атак на предприятия военно-промышленного комплекса и государственные учреждения в нескольких странах. Были атакованы более дюжины организаций, включая заводы, конструкторские бюро и НИИ, государственные агентства, министерства и ведомства нескольких стран Восточной Европы (Белоруссии, России и Украины), а также Афганистана. Часть вредоносного ПО, примененного в этих атаках, ранее отметилась в атаках APT-группы IronHusky. Эксперты также обнаружили вредоносное ПО и командные серверы, ранее использованные в атаках, которые другие исследователи атрибутировали APT-группе TA428.

Злоумышленники проникают в сеть предприятия с помощью тщательно подготовленных фишинговых писем, содержащих в том числе информацию, не доступную в публичных источниках. В новой серии атак они использовали сразу шесть разных бэкдоров (PortDoor, nccTrojan, Cotx, DNSep, Logtu и CotSam) — вероятно, для резервирования канала связи с зараженной системой на случай, если одна из вредоносных программ будет обнаружена и удалена защитным решением. Использованные бэкдоры предоставляют обширную функциональность для контроля над зараженной системой и сбора конфиденциальных данных. Финальным этапом развития атаки является захват контроллера домена и получение полного контроля над всеми рабочими станциями и серверами организации.

Получив права доменного администратора, злоумышленники приступают к поиску и загрузке документов и других файлов, содержащих конфиденциальные данные атакованной организации, на свои серверы, развёрнутые в разных странах. Эти же серверы используются как серверы управления вредоносным ПО. Злоумышленники помещали украденные файлы в зашифрованные ZIP-архивы, защищенные паролем, — возможно, с целью обхода решений класса DLP. После получения собранных данных серверы управления вредоносным ПО первого уровня пересылали полученные архивы на сервер управления второго уровня, расположенный в Китае.

Атаки APT31

В апреле 2022 года специалисты PT Expert Security Center обнаружили атаку на ряд российских энергетических и медиа-компаний, в которой использовался вредоносный документ. В ходе расследования были выявлены и другие документы, использованные в атаках на те же объекты. В кампаниях применялись одинаковые фрагменты кода для сбора информации о сетевых адаптерах и о зараженных системах. Прослеживалось явное сходство между использованными в атаках документами, и во всех случаях для управления вредоносным ПО использовались облачные серверы. Анализ примененного злоумышленниками инструментария показал, что в качестве командного сервера используется сервис Yandex.Disk.

Изученные образцы вредоносного ПО датируются периодом с ноября 2021 года по июнь 2022 года. Во всех случаях использовались легитимные файлы, основная задача которых — передать управление вредоносной библиотеке, используя, например, технику DLL Side-Loading, а также сформировать инициализирующий пакет для отправки его на командный сервер. Значительная часть обнаруженных легитимных исполняемых файлов оказались какими-либо компонентами Яндекс.Браузера и были подписаны действительной цифровой подписью. Анализ образцов вредоносного ПО показал, что за атакой стояла группа APT31.

Атаки TA423/Red Ladon

Proofpoint и команда исследователей PwC Threat Intelligence опубликовала совместное исследование о кампании кибершпионажа, нацеленной на государственные учреждения, энергетические и производственные организации в Азиатско-Тихоокеанском регионе. Злоумышленники рассылали фишинговые письма, содержащие ссылки, которые перенаправляли жертв на фальшивый новостной ресурс. Стоящая за атакой группа, которую авторы исследования называют TA423, Red Landon и APT40, использовала этот ресурс для доставки на компьютеры жертв вредоносного ПО, известного как ScanBox.

ScanBox устанавливает код на JavaScript либо единым блоком, либо, как в кампании апреля 2022 года, на основе модульной архитектуры, использующей плагины. Основная вредоносная нагрузка устанавливает конфигурацию ScanBox, включая информацию, которую надо собирать, и командный сервер, с которым следует установить соединение. В частности, собираются подробные сведения об используемом браузере.

Возможности дополнительных плагинов ScanBox, устанавливаемых у жертвы, включают функционал клавиатурного шпиона, формирование списка плагинов, используемых браузером жертвы, сбор подробных сведений о браузере жертвы (browser fingerprinting), установку однорангового соединения, — что дает возможность установки соединения с зараженным узлом через NAT и позволяет обойти сетевые экраны и другие защитные решения, установленные на том же сетевом устройстве, что и NAT (подробнее о векторе атаки смотрите в нашем блоге), — а также проверку, не установлено ли на атакованном компьютере защитное решение Kaspersky Internet Security (KIS).

Шпионаж за государственными организациями стран Азии

По сведениям Symantec, правительственные и государственные организации в ряде стран Азии атакованы с целью осуществления кибершпионажа группой хакеров, ранее замеченной в связях с троянской программой удаленного доступа ShadowPad. Злоумышленники используют широкий ассортимент легитимных программных пакетов для загрузки своих вредоносных нагрузок с помощью техники DLL side-loading.

Среди жертв вредоносной кампании государственные организации и СМИ, компании, работающие в сферах информационных технологий и телекоммуникаций, а также государственные аэрокосмические и оборонные компании.

В качестве вредоносной нагрузки используются утилиты для кражи информации, клавиатурные шпионы, скрипты PowerSploit, PlugX/Korplug, Trochilus RAT, QuasarRAT, общедоступные инструменты и т.д. Исследователям не удалось уверенно атрибутировать эти атаки, однако с ограниченной достоверностью прослеживается связь с более ранними атаками нескольких известных групп, включая Blackfly/Grayfly (APT41) и Mustang Panda.

Атаки Budworm

Исследователи Symantec опубликовали отчет с подробностями кампании кибершпионажа, цели которой включают правительство одной из ближневосточных стран, международную компанию — производителя электроники и законодательное собрание одного из штатов США. Считается, что хакерская группа Budworm имеет связи с правительством Китая.

По представленной в отчете информации, группа Budworm использовала уязвимости библиотеки Log4j (CVE-2021-44228 и CVE-2021-45105) в недавних атаках, в ходе которых на серверах взламывается служба Apache Tomcat для установки веб-шеллов на атакованные системы. Злоумышленники использовали в качестве командных серверов виртуальные частные серверы (Virtual Private Servers, VPS), размещенные на хостингах Vultr и Telstra. Кроме HyperBro, который использовался в качестве основного инструмента, в арсенале злоумышленников присутствовали и другие инструменты, такие как CyberArk Viewfinity, Cobalt Strike, LaZagne, IOX, Fast Reverse Proxy и Fscan.

Атаки Earth Longzhi

Согласно исследованию Trend Micro, ранее неизвестная подгруппа группы APT41 (она же Winnti) атаковала организации в Восточной и Юго-Восточной Азии и Украине как минимум с 2020 года.

Целями первой волны атак группы, получившей название Earth Longzhi, были государственные организации, инфраструктурные компании и компании здравоохранения Тайваня, а также банки Китая. В ходе второй волны атак жертвами группы стали важные объекты в Украине, а также нескольких азиатских странах, включая оборонные, авиационные, страховые и градостроительные компании.

В обеих кампаниях целенаправленные фишинговые рассылки использовались в качестве вектора первоначального заражения вредоносным ПО Earth Longhzhi, которое содержалось в запароленном архиве или загружалось по ссылке на Google Drive, ведущей на запароленный архив. В обоих случаях в архиве содержался нестандартный загрузчик Cobalt Strike.

Для этапов атаки, следующих после проникновения в атакуемую систему в ходе одной из кампаний, группа Earth Longzhi подготовила комплексный инструмент, сочетающий в одном пакете все необходимые средства атаки, включая прокси, сканер портов, сканеры паролей и т.д. Большинство инструментов, включенных в комплексный пакет, общедоступны или применялись в предыдущих атаках. В ходе расследования второй кампании были обнаружены несколько хакерских инструментов, предназначенных для повышения привилегий в системе (PrintNightmare и PrintSpoofer), кражи учетных данных (нестандартный автономный вариант Mimikatz) и ухода от средств защиты (отключения защитных продуктов). Злоумышленникам удалось заново реализовать или разработать собственные инструменты на основе проектов с открытым исходным кодом.

Активность русскоговорящих групп

Атаки IRIDIUM/Sandworm

В октябре исследователи Microsoft опубликовали отчет о новой программе-вымогателе, названной Prestige, нацеленной на транспортную и логистическую отрасли Украины и Польши. Первоначально вредоносной программе было дано временное имя DEV-0960. Отмечается частичное совпадение жертв вредоносных программ Prestige и HermeticWiper, однако неясно, стоит ли за обеими вредоносными программами одна и та же группа злоумышленников DEV-0960. Активность DEV-0960, предшествующая установке программы-вымогателя, включала применение утилиты RemoteExec и утилиты с открытым исходным кодом Impacket WMIexec. В некоторых из атакованных организаций, чтобы получить доступ к учетным данным аккаунтов с высоким уровнем привилегий, группа DEV-0960 использовала утилиту с открытым исходным кодом winPEAS, предназначенную для повышения привилегий в системе, инструмент для создания дампа памяти процесса LSASS и кражи учетных данных, а также инструмент для создания резервной копии базы данных Active Directory. В ноябре исследователи MSTIC researchers опубликовали обновление блог-поста, в котором атрибутировали атаку группе злоумышленников IRIDIUM (она же Sandworm, Hades).

Атаки Cloud Atlas/Inception

Исследователи из компании CheckPoint проанализировали серию атак, проводимых группой Cloud Atlas (она же Inception) с июня 2022 года. Атаки направлены на очень узкий круг целей в Беларуси, прежде всего в секторах транспорта и военной радиоэлектроники, а также в России, в таких отраслях как органы государственной власти, энергетика и металлургия. Кроме того, активность группы по-прежнему направлена на Крымский полуостров, Луганскую и Донецкую области. Cloud Atlas уже много лет использует в качестве первоначального вектора атаки целенаправленные фишинговые рассылки с вредоносными вложениями. В качестве приманки используются текущие геополитические проблемы, актуальные для страны, где находятся цели атаки. В большинстве случаев фишинговые письма отправляются через публичные почтовые сервисы, такие как Yandex, Mail.ru и Outlook.com, однако иногда группа делает попытки подмены доменов, используя домены, которые, скорее всего, вызовут доверие потенциальной жертвы. На следующем этапе атаки Cloud Atlas, как правило, использует бэкдор PowerShower на основе PowerShell.

Исследователи из компании Positive Technologies также опубликовали отчет об активности группы, в котором добавили новые подробности о странах, в которых группа атакует органы государственной власти, а также об используемых ей схемах атак и инструментарии.

Другие атаки

Атаки Woody Rat

Команда Malwarebytes Threat Intelligence обнаружила ранее неизвестную троянскую программу для удаленного доступа и дала ей название Woody Rat. Данный троянец существует в дикой среде не меньше одного года. Этот нестандартный троянец с продвинутым функционалом по большей части применяется группой, которая атакует цели в России, используя файлы-приманки архивных форматов (имена файлов “anketa_brozhik.doc.zip” и “zayavka.zip”), а в последнее время и документы Office (“Памятка.docx”). При этом используется уязвимость Follina (CVE-2022-30190). По мнению исследователей, группа, стоящая за Woody RAT, атаковала российскую аэрокосмическую и оборонную организацию ОАК с использованием фальшивого доменного имени, зарегистрированного злоумышленниками. На данный момент у исследователей нет надежных сведений, позволяющих атрибутировать эту кампанию определенному актору.

Атаки Worok

Исследователи компании ESET обнаружили целевые атаки на известные компании и местные органы власти преимущественно в странах Азии, но также на Ближнем Востоке и в Африке. Атаки проводились ранее неизвестной группой, ориентированной на кибершпионаж, которая активна как минимум с 2020 года. Исследователи назвали группу “Worok”. Цели атак группы включают компании из различных отраслей — телекоммуникации, банки, морское судоходство, энергетика, органы государственной власти и государственные организации. В некоторых случаях группа Worok использовала для получения первоначального доступа печально известные уязвимости ProxyShell. После получения доступа операторы проводили разведку с помощью нескольких общедоступных инструментов, включая Mimikatz, EarthWorm, ReGeorg и NBTscan, а затем переходили к развертыванию собственных нестандартных имплантов: загрузчика первого этапа, затем загрузчика .NET второго этапа (PNGLoad). Финальную вредоносную нагрузку исследователям получить не удалось.

Исследователям компании Avast удалось расширить описание схемы компрометации, используемой группой. Они подтвердили, что группа использует стеганографию, с помощью которой прячет вредоносное ПО в изображения PNG. Используемый злоумышленниками метод первоначального заражения остается неизвестным, однако исследователи считают, что актор, вероятно, использует технику DLL side-loading для выполнения в памяти загрузчика вредоносного ПО CLRLoader. Таким образом загружается DLL второго этапа PNGLoader, которая извлекает байты, зашифрованные в файлах PNG, и собирает из них две вредоносных нагрузки. Первая вредоносная нагрузка — это скрипт PowerShell. В распоряжении исследователей пока нет образца этой вредоносной нагрузки, однако, предположительно, она имеет такой же функционал, что и вторая вредоносная нагрузка, которая представляет собой .NET бэкдор, написанный на C#. Она называется DropBoxControl и предназначена для взаимодействия со злоумышленниками через службу DropBox. Жертвы этой кампании, описанные исследователями Avast, имеют много общего с теми, что описаны в отчете ESET. В их число входят компании и государственные учреждения в Азии (во Вьетнаме и Камбодже) и Северной Америке, в частности, в Мексике.

Бюллетени CISA

APT-группы с поддержкой Ирана

CISA (Агентство по кибербезопасности и безопасности инфраструктуры США), ФБР, АНБ (Агентство национальной безопасности США), Киберкомандование США — Национальная кибернетическая группа (U.S. Cyber Command, USCC — Cyber National Mission Force, CNMF), и Федеральное казначейство США опубликовали совместный бюллетень безопасности об атаках APT-групп, связанных с Корпусом стражей исламской революции (КСИР) Ирана, на широкий круг организаций, включая организации в различных секторах критической инфраструктуры США. В подготовке бюллетеня безопасности участвовали также агентства по кибербезопасности Австралии, Канады и Великобритании. Этот новый бюллетень является обновлением бюллетеня, опубликованного в ноябре 2021 года, в котором содержится информация об атаках тех же APT-групп с использованием уязвимостей в продуктах Microsoft, Fortinet и ProxyShell. Помимо ранее известных уязвимостей, арсенал этой группы пополнился уязвимостью в VMware Horizon Log4j, которая используется для получения первоначального доступа к целевым средам. APT-группы используют этот первоначальный доступ для реализации вредоносной активности, такой как

шифрование дисков и кража конфиденциальных данных с целью получения выкупа. Агентства, принявшие участие в подготовке бюллетеня безопасности, призывают организации, в особенности «организации критической инфраструктуры», использовать представленный в бюллетене список мер для минимизации риска компрометации в результате атаки данной APT-группы.

Взлом систем оборонного подрядчика

В совместном бюллетене CISA (Агентства по кибербезопасности и безопасности инфраструктуры США), ФБР (Федерального бюро расследований) и АНБ (Агентства национальной безопасности США) сообщается, что в течение периода с ноября 2021 года по март 2022 года злоумышленники осуществляли скрытный доступ к сети организации военно-промышленного комплекса США и осуществляли кражу конфиденциальных данных. В бюллетене CISA представлены технические подробности реагирования на данный инцидент. Было обнаружено, что, по всей вероятности, сеть организации была скомпрометирована несколькими APT-группами, причем некоторые из них имели доступ к сети в течение продолжительного времени. Злоумышленники взломали сервер Exchange организации и использовали взломанную учетную запись администратора для отправки запросов на сервер Exchange через API EWS. Они также использовали набор сетевых утилит с открытым исходным кодом Impacket для удаленного управления компьютерами и развития атаки.

Центр реагирования на инциденты информационной безопасности промышленных инфраструктур «Лаборатории Касперского» (Kaspersky ICS CERT) — глобальный проект «Лаборатории Касперского», нацеленный на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур.

Kaspersky ICS CERT ics-cert@kaspersky.com